WATER SYSTEM SECURITY GUIDANCE DOCUMENT

MICHIGAN SECTION AWWA

RESEARCH & TECHNICAL PRACTICES COMMITTEE

SECURITY SUBCOMMITTEE

JULY, 2002

TABLE OF CONTENTS

WATER SYSTEM SECURITY GUIDANCE DOCUMENT

This document was developed to provide guidance and direction to water utilities relative to water system security issues. As each utility is different and has unique vulnerabilities, it is important to consider other available resources and to consult with various security experts before implementing specific measures to meet your needs.

This document was produced in 2002 by the Water System Security Subcommittee of the Research & Technical Practices Committee, Michigan Section AWWA.

Subcommittee members include: Dennis Benoit, Rolf Deininger, David Koch, Michael Kovach, William Maier, Kimberly Mason, David McKay, Thomas Newhof, Timothy LeTourneau, David Timm (Chair), John Wierenga

Michigan Section AWWA
Water System Security Position Statement
July, 2002

Safe, adequate, and reliable water supplies are essential to Michigan's economy, and the health and safety of its citizens. Through great diligence, Michigan water utilities have historically provided this service with little disruption. However, terrorism represents a new and potentially serious threat to the water supply industry, to which we must now respond. While the likelihood of such an incident may be small, the threat is real and the consequences could be serious. The threat of terrorism is only one reason for a renewed emphasis on water utility security.

It of course must be recognized that standard utility practices already provide numerous safeguards which serve to minimize various threats. These safeguards include source water protection efforts, multiple barrier treatment schemes, water quality monitoring programs, system redundancies, diligent and competent operators, etc. Again, these efforts have served us well, and while not necessarily provided in response to terrorism, certainly serve to reduce associated risks. However, additional security efforts are warranted to minimize terrorist threats to our industry, and enable us to continue to meet our objectives.

Based on the above, the Michigan Section AWWA encourages all Michigan water utilities to review the risks and liabilities associated with their facilities, and as necessary and where applicable:

- Conduct a comprehensive vulnerability assessment of their facilities;
- Provide necessary enhancements;
- Review and update emergency management plans and procedures to enable prompt and appropriate response should an incident occur;
- Incorporate security enhanced designs when considering facility upgrades or expansions.

To assist with these efforts, the Research and Technical Practices Committee has developed the attached security related guidance materials, which are adopted as part of this Position Paper. These documents pertain to: vulnerability assessments, security enhancements, response activities, and design considerations. By following a systematic approach to security issues, utilities can help ensure that their resources are used in a responsible manner to address their unique vulnerabilities.

VULNERABILITY ASSESSMENTS

Utility security is not necessarily about buying the latest electronic gadgets. Nor is it about creating an impenetrable fortress out of your facility. More objectively, a utility manager should utilize a Risk-Management Perspective in addressing security by performing an Asset-Based Vulnerability Assessment (VA). By doing so, managers can prioritize facilities determined to represent the highest risk, and then ensure the level of security provided is appropriate for the degree of risk represented.

The goal of security systems and procedures is to minimize your overall risk and liability. Before you begin a VA, you may wish to consider the possibilities by *Identifying Threats.* Threats may be associated with Vandalism, Contamination, Severe Weather Events, or other Disruptions. Threats can also be carried out by terrorists, other criminal agents, extremist groups, insiders, or nature.

The *first step* in performing a VA is that of *Asset Identification.* Begin by identifying facilities, i.e., make a list of what you have. Facilities can be intakes, wells, treatment plants, pump stations, reservoirs, transmission mains, operational control centers, supply/service yards, hydrants, or any other component of a water system.

The second *step* in performing a VA is *Determining the Levels of Risk Present.* Determining Risk can be broken down into three (3) areas, including the following:

a. Determine **Vulnerability.** How safe/exposed is an asset? Is your WTP located in a remote, rural area, or in a high-density urban setting? What are the countermeasures already in place? Is your WTP chorine storage area fenced? Accessible to traffic? Do you already have door locks and cameras in place?

b. Determine **Criticality** (Consequences). Consequences can range from localized service disruptions to system contamination. How critical is a particular asset to your operation? If a particular pump station is taken out of service, can water be delivered by another station or tower? Is it critical that a particular asset remain in service at all times?

c. Determine **Probability**. What is the likelihood of an event occurring to an asset? For example, what are the chances of a lake intake five (5) miles offshore being disrupted? How likely is it that your identified asset will be impacted?

The *third step* in performing a VA is *Quantifying Levels of Risk.* Risk can be identified as the formula: V x C x P where V = Vulnerability, C = Criticality, and P = Probability. You may assign any numerical scale you desire. An asset may be highly vulnerable, say 0.9 on a 0 to 1 scale, however, it may score low on criticality and probability, say 0.1 each. Therefore, the overall risk, 0.009, out of a possible 1.0, is low. Compute numerical Risk Levels for each asset.

The *fourth step* in a VA is *Determining Risk Acceptability.* By evaluating the Risk Levels calculated, determine the level of risk acceptable for your system.

It is important to realize that the VA can be approached in a number of ways. A VA can be self-performed by utilizing your existing staff. A VA can also be performed by qualified design engineers as well as experienced security firms. Consideration should be given by other agencies such as first responders like local police and fire departments. An independent look at your facilities is encouraged.

SECURITY ENHANCEMENTS

Security enhancements will not guarantee that damage or entrance to a facility will not take place, but should be viewed as a means to both **Deter** and **Detect** potential threats. Ideally, this combination of detection and deterrence will provide sufficient time for an appropriate **Response** to prevent serious consequences. These enhancements may involve several venues for water plants, wells, water inlets or distribution facilities for prevention from vandals, or terror threats. Well-trained experienced professionals, familiar with water utility operations and service procedures, should be used to make a full security assessment to determine which venues may be effective.

Once the assessment is completed, recommended enhancements may include a variety of equipment and facilities, along with operational modifications. Materials or products utilized should **NOT** be of general-purpose quality. Utility providers should incorporate the "belt & suspenders" approach to all security systems.

Some suggestions for security measures include:

EQUIPMENT/FACILITIES:

A. **Physical Barriers**: Where security fence is allowed or required, only the commercial grade chain-link fence should be used. A minimum fence height of 8 ft. or 10 ft. where there is no height restriction with three strands of barbed wire or razor wire is recommended. Fencing should be arranged to prevent gaining entrance from under the fence or from a structure or landscaping close to the fence. Stringing a ¾-inch cable within the fence can be considered to provide an additional barrier to vehicles. Other types of physical barriers such as concrete pylons, brick or concrete walls, and trenches or moats should also be considered where appropriate. Barriers may be appropriate around chemical storage areas, electrical substations, fuel containment areas, reservoirs, pumping stations, and remote facilities.

B. **Lighting**: High-pressure sodium or metal halide lights utilizing 400 to 1000 watts should be the standard. These bulbs will have fewer shadows and remain brighter over the life of the bulb. Where necessary, vandal proof lenses and reflectors could also be used. Extra lighting requirements should be noted in areas where there is limited staffing, chemical or fuel storage.

C. **Windows**: All windows and door glass should meet the "security glass" requirements. This may include the metal mesh in the glass itself or non-breakable glass.

D. **Doors, Keys and Locks**: Entrance doors should be locked at all times. All doors should be of commercial grade metal including frames. The door hinge should be hidden from the outside to prevent removal of hinge pins. Door locks should be a "dead-bolt" type. This could include the type where the key can't be removed unless the lock is locked. This generally prevents the door from being left unlocked by a forgetful operator. Doors, which must be locked, and not attended on a full-time basis, where the public will enter, should have a doorbell or other notification means.

A "card entrance" system allows the **Utility** to keep track of which employee enters and when. The system also permits immediate cancellation of authority to enter by a discharged or retired employee without a significant expense of changing locks.

Several other areas may require a second dead-bolt lock system with only authorized personnel having keys or an additional "card-swipe" station. However the "card-swipe" station is more expensive. Only commercial grade lock systems should be used at all locations.

Key distribution is an important part of security. All keys should be labeled. **"DO NOT DUPLICATE". HOWEVER -** Don't trust this for security.

You should provide your local police or security agency with a passkey for immediate entrance in case of an emergency, to conduct an immediate surveillance search or to apprehend an individual.

E. **Signage/ I.D.**: Signage is extremely important to inform workers and especially the public which areas they are authorized to enter. Signage may also provide building or area identification and emergency phone numbers for reporting purposes and to provide quick information for responding agencies. Identification badges should be provided to staff, visitors, and contractors indicating their authorization to be in the facility, or which portion of the facility they are allowed in.

F. **Vents, Access Ports & Overflows:** Stainless Steel bars or a "dog house" structure preventing access should protect all of these types of areas.

G. **Padlocks**: Every access port, vent or gate should be protected with a "high security" type pad lock. These are made of high tensile steel and/or have limited access to shackles.

H. **Building Interior Security: Motion and noise detectors are essential. They may be as simple as a loud, suggested 120 db, indicator or connected to an emergency response agency. These should be tested monthly. At remote facilities, it may be appropriate to have pumping units automatically shut down whenever an intrusion alarm is activated.**

I. **Security Cameras: Some areas may require security cameras. These may appear to be effective, however they require constant vigilance. They are important as a means to recording who was involved in an incident.**

J. **Tamper-Proof Devices: Consider utilizing tamper-resistant hydrant caps, valve box lids and manhole covers where appropriate.**

OPERATIONS:

A. **Water Quality: Carefully monitor and evaluate daily operational parameters such as pH, disinfectant demand and residual levels, to assist in detecting unusual chemical or biological conditions that might identify vandalism, tampering, or an intentional contamination attempt. Consider on-line instrumentation to detect changes in water quality, pressure or flow at various locations, including various distribution system sites.**

B. **Inspections: Provide frequent scheduled and unscheduled inspections of water supply facilities and note anything unusual. Request that local law enforcement officials include your facilities in their surveillance efforts.**

C. **Neighborhood Watch**: Adjacent residential, commercial or industrial neighbors should be encouraged to report any unusual activities.

D. **Vehicles**: Unattended vehicles should be locked to prevent them from being stolen or used as a drivable ram through a fence or into a building.

E. **Deliveries**: Verify all deliveries and require appropriate identification from delivery personnel. Chemical deliveries to water plants should receive extra scrutiny (see Chemical Security Delivery Checklist in Appendix A).

F. **Hydrants, Valves, Cross Connections**: Ensure that hydrants and valves are in proper working order as they are often critical during emergency situations. Have accurate system maps to assist in rapid response. Maintain a strong cross connection control program to minimize potential avenues of contamination.

G. **Computers/SCADA**: Update anti-virus software, limit access, change passwords routinely, and install firewalls.

H. **Power Supply**: Ensure that backup power is available. Routinely exercise generators, switch gear, and controls to ensure their dependability.

I. **Contingency Plans**: Ensure that contingency plans have been updated and are available to staff. Identify emergency phone numbers, a chain-of-command, policies and procedures for responding to emergencies.

J. **Communications**: Establish communication links with local emergency planning officials, emergency responders, local police, public health officials, local hospitals, the media and others who may be involved should an emergency situation arise. Ensure that a variety of communication equipment can be utilized to maintain control systems and enable effective response during an emergency – radios, cell phones, land line phones, etc.

K. **Background Checks**: Conduct security background checks on employees at hiring and periodically thereafter. Similar checks should be conducted on contractors.

L. **Training**: Encourage staff to note and report anything suspicious. Make sure they are aware of policies and procedures to be followed pertaining to security measures and response activities. Conduct mock drills to enhance training and coordination activities.

M. **FOIA's/Public Information**: Minimize disclosure of information that could jeopardize water system security. Sensitive information could include water system maps, vulnerability assessments, security plans, contingency plans, etc.

SECURITY RESPONSE PROCEDURES

The following is an outline of recommended security response procedures water utilities should follow in the event of a perceived threat to the security of the water supply system. These procedures should be part of the community's local emergency response plan.

A. Water utility personnel or other city officials receiving a telephone call threat or other threat notification about the water supply system should try to attain as much information as possible about the caller and/or the nature of the threat. Use of the telephone log outline in Appendix B to record event details is strongly recommended.

B. Following receipt of a threat to the water supply, municipal officials must determine the credibility of the threat through review of available records and/or on-site investigation of respective facilities. Local law enforcement officials must be notified at once and accompany water department personnel to observe those areas where entry/intrusion may have occurred.

C. Increased water quality monitoring may be appropriate depending on the frequency and type of routine monitoring being carried out. Augment routine monitoring with tests that are most likely to uncover the presence of suspected contaminants. Whether or not contamination is confirmed, establish and maintain a formal record of time, date and location of tests, and indicate that the tests are in response to a particular instance of a suspected breach of security. These records may prove to be valuable in future investigations.

D. Water utility officials must notify the Michigan Department of Environmental Quality (MDEQ) Drinking Water and Radiological Protection Division (DWRP) District Engineer within one business day of a suspected breach of security that may have compromised the provision of safe drinking water to customers.

E. If there are no credible indications of entry into or breaching of security for the water supply system, and there are no indications of the introduction of foreign agents having been introduced into the water system, water utility officials should resume normal system operation.

F. If a breach of water system security is suspected or is confirmed, water utility and local law enforcement officials should contact other agencies, such as the FBI and MDEQ, to assist with on-site investigations. (see EPA Emergency Notification Protocols in Appendix C).

G. As soon as possible, an assessment of the magnitude of the overall threat must be made. All efforts must be quickly put forth to isolate the affected area or areas of the distribution system/treatment/storage facilities and curtail the spread of possible contaminants.

H. If water quality is at risk, appropriate notification to customers as to precautionary measures must be issued as soon as possible. Local media, government officials and public health departments should be alerted to the potential risk and actions to be taken. A spokesperson who represents both the water utility and health department should perform all communication to the public and media.

I. Water quality analyses of samples from the potentially affected area should be carried out by agencies experienced in addressing water system security threats. Water suppliers should contact the MDEQ at 1-517-241-1300 for a listing of these agencies (after hours, contact 1-800-292-4706).

J. If the contaminant is a hazardous substance or is unknown, local hazardous substance management personnel should initiate appropriate clean up measures as soon as practical.

K. Depending on the duration of interruption to normal water service, the water utility should make provisions to provide an alternate source of drinking water to water customers. Instructions to alert water customers about the availability of the alternate drinking water source should be provided in the public notice (see Item H).

L. Once the water system facilities have been rid of possible contaminants, appropriate water quality sampling must be carried out to confirm restoration of normal water quality.

M. Following receipt of satisfactory water quality analyses, notice to water customers must be issued announcing resumption of normal usage.

N. Water suppliers may find it beneficial to maintain an inventory of appropriate sampling containers to facilitate water quality monitoring following a reported incident.

DESIGN CONSIDERATIONS

In the design of new facilities, evaluation of existing facilities, and retrofit and expansion of existing facilities, water supply systems should take appropriate measures to provide for an adequate level of safety of the water supply from acts of terrorism. Key issues for analysis in review of planning/design for facility improvements are described below.

Protection of the facilities that produce, treat, store, and transport water:

A. Redundancy of supply, treatment, and distribution.
1. Is an alternate source of raw water supply available?
2. Are there any single points of process flow from the water supply through the treatment system?
3. Can parallel units be isolated?
4. Do sufficient interconnects, and does adequate valving exist between parallel units and upstream and downstream units?
5. Is an alternate source of power available?
6. Is manual control and operation available upon loss of automated system?

B. Protection of water distribution and storage facilities, whether attended, unattended, central or remote, from the introduction of contaminants or other substances.
1. Are hatches and other access means protected from entry or tampering?
2. Are facility vent and overflow connections adequately protected?
3. Do hydrants have tamper-proof caps?
4. Are chemical delivery systems provided with means of sampling prior to acceptance into plant storage?

C. Protection of water supply, treatment, and distribution facilities from intrusion by unauthorized personnel.
1. Are facilities adequately fenced or otherwise secured?
2. Are doors and other access points locked against external access?
3. Are other access control devices/systems warranted (e.g., key card access, video monitoring, intrusion alarms, motion detectors)?
4. Are windows subject to entry, and if so, are they protected from such (e.g., wire mesh, alarms)?
5. Is site/exterior lighting adequate?

D. Protection of the raw water supply via appropriate source water protection measures.
1. Has a source water assessment been completed?
2. For reservoir sources, is the reservoir subject to other public use, and if not, is it properly fenced?
3. For groundwater sources, has an aquifer/wellhead protection program been implemented?
4. For well supplies, are all wells or well houses adequately fenced, locked, or other wise protected?

E. Protection of support systems for operation and monitoring of water treatment and distribution.
   1. Is SCADA/network system protected via firewalls?
   2. Is access to SCADA/network restricted via passwords?
   3. Are multiple modes/routes of communication provided to remote sites?
   4. Are uninterruptible power supplies (UPS) provided for control systems?

F. Providing adequate horizontal clearance from public rights-of-way for critical components.
   1. Does the location of key facilities provide for a suitable buffer zone from public rights-of-way?
   2. Can physical barriers be installed for further protection?

G. Evaluation of unattended facilities in terms of accessibility and monitoring.
   1. Is the operation of remote unattended facilities monitored?
   2. Do the restrictions on access also restrict periodic visual monitoring?

Protection of the source and product water:

A. Protection of the raw water supply via monitoring of the raw water supply.
   1. Is the source water monitored on-line prior to introduction to the treatment plant?

B. Compliance with treatment and finished water regulations.
   1. What improvements are required to ensure compliance?

C. Consideration of remote on-line monitoring stations in the transmission/distribution system for disinfectant residual, toxics, or appropriate indicators.
   1. Can on-line monitoring be implemented at key locations?

Provisions for responding/reacting to acts of terrorism or other major service interruption:

A. Means of emergency supply in event of catastrophic loss of supply or treatment.
   1. Are interconnects provided, and operable, to neighboring water supply systems?
   2. Are facilities provided to allow a temporary connection by alternate means to the distribution system in an emergency situation (e.g., bypass of treatment plant)?

APPENDIX A

CHEMICAL DELIVERY SECURITY CHECKLIST

1. Vendors send the utility, photos and names of drivers making deliveries.

2. Prior to making a specific delivery, vendor provides utility with name of driver before truck leaves the terminal. This enables utility to match up the driver and photo with his/her I.D. when the truck arrives.

3. Trucks will be sealed with a security tag, and the serial number will be faxed to the utility after the truck has been loaded and is ready for shipping.

4. The tanker number will also be faxed to the utility in order to match the numbers, assuring it is the same tanker that left the terminal.

5. The utility will use two staff members on a regular basis to offload chemicals. This way they will become familiar with procedures, drivers, manifests, etc.

6. The manifests will contain information pertaining to the delivery along with the serial numbers and tanker numbers.

7. Plant operators will notify supervisors of any discrepancies before proceeding with the offloading process. Discrepancies will result in delay of chemicals being offloaded until they can be resolved. Ultimately, discrepancies could result in shipments being refused.

8. The Police Department and/or FBI should be notified in the event of significant differences.

This checklist was adapted from that contained in "Guarding Your Drinking Water", Maryland Center for Environmental Training

APPENDIX B

TELEPHONE LOG FOR RECORDING THREATS

If your utility receives a threatening phone call, try to keep the caller on the line to obtain as much information as possible. Record as much information as possible, including:

1. What kind of threat is posed?.
   a) Contamination: What kind of poison? ______________________________
   How much? ______________________________
   b) Physical Damage: What kind of damage? ______________________________
   With what kind of device?______________________________
2. Where? ______________________________
3. When? ______________________________
4. Why? ______________________________
5. By Whom? ______________________________
6. What is your (caller's) name? ______________________________
7. What is your (caller's) affiliation, if any? ______________________________
8. What is your (caller's) address/phone #? ______________________________
9. What is the exact wording of the threat? ______________________________
10. Is the caller__male__female__well spoken__illiterate__foul__irrational__incoherent
11. Is the caller's voice__calm__angry__slow__rapid__soft__loud__laughing__crying
    __normal__slurred__nasal__clear__lisping__stuttering__deep__high__cracking
    __excited__young__old
    __familiar – who did it sound like? ______________________________
    __accented – what nationality, region? ______________________________
12. Is the connection clear?(Could it have been a wireless or cell phone)______________
13. Are there background noises?__street noises – what kind? ______________________
    __machinery – what type?______________________________
    __voices – describe______________________________
    __children – describe______________________________
    __animals – what kind?______________________________
    __computer keyboard/office______________________________
    __motors – describe______________________________
    __music – what kind?______________________________
    __other______________________________

Name of person receiving call______________________Date__________Time__________
Notify Utility manager______________________________phone:____________________
Local FBI/Law Enforcement, Phone:______________________________
Other______________________________phone:______________________________

APPENDIX C

EPA EMERGENCY NOTIFICATION PROTOCOLS

EPA Water Protection Task Force

Notice #VIII: Emergency Notification Protocols
February 21, 2002

This document contains security information that is considered sensitive and is intended solely for water system staff and representatives. Please do not distribute publicly or share with the media.

What is this Notice?

This notice provides suggestions for the development and coordination of water utility emergency notification protocols, a critical aspect of incident response and management. Differences between state and local requirements make it difficult to develop uniform notification procedures applicable to all localities and states. The following suggestions for developing emergency notification protocols at the local level are oriented toward an incident involving a terrorist or other intentional act that threatens to disrupt the water system (wastewater and drinking water) or that otherwise impacts the safety of drinking water. An intentional act to disrupt the operations of a water utility or to jeopardize public health is a criminal act that creates the need to notify the appropriate FBI field office, National Response Center and other entities that may not normally be contacted in response to a natural disaster or emergency.

Water utilities that have established notification procedures to meet a regulatory requirement, such as the Emergency Planning and Community Right-to-Know Act (EPCRA), should use them as the starting point for developing broader notification procedures. Utilities that do not have established notification procedures should work with their Local Emergency Planning Committee (LEPC) or similar local/state emergency planning organization, prior to an incident, to coordinate the specific procedures for contacting local, state and federal officials when an incident occurs. You can find LEPC for your location at http:www.epa.gov/lepclist.htm.

Notification Protocols

The notification procedures developed within the local coordination effort should provide agency-specific names and contact numbers for emergency notification on a 24-hour basis. The protocol should define what information about the incident needs to be provided, identify which authorities need to be notified and specify the notification responsibilities for each local government agency.

EPA suggests that the utility first call local law enforcement officials to initiate local emergency response actions. This may be accomplished by calling 911 or a direct call to local law enforcement. The local notification protocol should determine which additional emergency response and management agencies (fire, emergency medical services (EMS), the community emergency management organization and state agencies) need to be notified. For instance, do fire and EMS need to be notified in addition to law enforcement for a water-related incident, or would one call to 911 serve to notify all? The local coordination effort should also consider procedures for notifying local and state health and environmental authorities, local critical care facilities (hospitals, dialysis centers, etc.) and others as identified in state and local requirements. EPA also suggests that the protocol ensure that all entities listed below are notified. The list is not all-inclusive and is not listed in any particular order of priority.

- Notify local law enforcement
- Notify local FBI Field Office (to begin the threat assessment process). Your local FBI Field Office can be located by visiting http:www.fbi.gov/contact/fo/info.htm or in the front pages of your local telephone book
- Notify National Response Center 1-900-424-8802 (to notify pre-determined federal response agencies). For more information on NRC see http:www.nrc.uscg.mil
- Notify state/local emergency management organization
- Notify the Governor's Office
- Notify other associated system authorities (wastewater, water)
- Notify local government officials (responsible authority for the water utility)
- Notify state/local health, water and/or environmental department
- Notify critical care facilities
- Notify employees
- Notify EMS and Fire Department as deemed necessary
- Consider when to notify customers and what notification to issue

Water utilities should specifically identify who within the utility has responsibility for making the notifications that the water utility is responsible for making.

For more information please contact the Water Protection Force at **protection.water@epa.gov**

APPENDIX D

ADDITIONAL RESOURCES:

American Water Works Association, *Water System Security: A Field Guide* (book, cat. no. 20501; video, cat. no. 65247); www.awwa.org/bookstore.

American Water Works Association, *Counter Terrorism and Security in the Water Industry: A Manager's Guide to Keeping Your Utility Safe* (workshop participant manual); www.awwa.org.

American Water Works Association, *Design of Early Warning and Predictive Source Water Monitoring Systems* (cat no. 90878); www.awwa.org/bookstore.

American Water Works Association, *Elevated Water Storage Tank: Safety and Security* (video, cat. no. 65193); www.awwa.org/bookstore.

American Water Works Association, *New Horizons: Critical Infrastructure Protection* (video, cat. no. 65226); www.awwa.org/bookstore.

Ginley, D.; "Technology Solutions for Physical Plant Security"; Journal AWWA (February 2002), Volume 94, No. 2: 46-48.

Great Lakes Upper Mississippi River Board of State Public Health and Environmental Managers, *Recommended Standards for Water Works* (Ten States Standards); 2002 (publication pending); www.hes.org.

American Water Works Association, *Emergency Planning for Water Utilities: Manual of Water Supply Practices M19* (cat no. 30019); www.awwa.org/bookstore.

Garcia, Mary Lynn – Sandia National Laboratories, *The Design and Evaluation of Physical Protection Systems*, (2001), Butterworth-Heinemann

United States Environmental Protection Agency, *Guidance for Water Utility Response, Recovery & Remediation Actions for Man-made and/or Technological Emergencies*, (April 15, 2002)